Serial No. ~~09/048,421~~ 09/957,421

REMARKS

Claims 1-15 stands rejected under 35 USC §101 as being directed to non-statutory subject matter. Claims 1-20 stands rejected under 35 USC §103(a) as being unpatentable over Apperson et al., U.S. patent 5,978,484 in view of Atkinson et al., U.S. patent 5,892,904.

Claims 1-15 have been amended to more clearly state the invention. Reconsideration and withdrawal of the rejection of claims 1-15 under 35 USC §101 is respectfully requested. In view of claims 1-15, as amended, applicants respectfully submit that the subject matter is statutory. Reconsideration and allowance of each of the pending claims 1-20, as amended, is respectfully requested.

Apperson et al., U.S. patent 5,978,484 discloses a method and system for distributing and executing executable code. Before sending executable code to a client, a distributing authority associates a privilege request code with the executable code. The privilege request code indicates a requested set of privileges that the executable code will potentially exercise during execution. The distributing authority digitally signs the executable code and associated privilege request code and then distributes it for eventual execution by clients. Before executing the executable code, a client verifies the digital signature to confirm the authenticity and integrity of the executable code and associated privilege request code. This verification utilizes a hierarchy of certifying authorities. While the code executes, the client monitors it and prevents it from exercising privileges that are not in the requested set of privileges.

Atkinson et al., U.S. patent 5,892,904 discloses a certification or signing

-8-

Serial No. 09/957,421

method to ensure the authenticity and integrity of a computer program, an executable file, or code received over a computer network. The method is used by a publisher or distributor to "sign" an executable file so it can be transmitted with confidence to a recipient over an open network like the Internet. The executable file may be of any executable form, including an executable or portable executable .exe file format, a .cab cabinet file format, an .ocx object control format, or a Java class file. The code signing method assures the recipient of the identity of the publisher as the source of file (i.e., its authenticity) and that the file has not been modified after being transmitted by the publisher (i.e., the integrity of the file). As a result, the code signing method allows an executable file to be transmitted over open computer networks like the Internet with increased certainty in the identity of the source of the file and minimized risk of contracting a computer virus or other malicious executable computer files.

Reconsideration and allowance of each of the pending claims 1-20, as amended, is respectfully requested.

As recited in independent claims 1, 7, and 16, as amended, the present invention teaches and claims a core product load manifest, a computer implemented method, and computer program product for protecting ongoing system integrity of a software product having a plurality of pieces using digital signatures.

The present invention as recited in independent claims 1, 7, and 16, as amended, solves an existing problem of protecting ongoing system integrity of a software product that requires that product software updates, a changed program replacing a program originally in the software product, and deleting or adding of a

-9-

Serial No. 09/946,421/471

program in the software product be accommodated.

The combined teachings of Apperson et al. and Atkinson et al. reflect the present state of the art, where protection typically includes protecting each piece, such as a program, with a digital signature of encrypted hash or checksum that can later be verified. The combined teachings of Apperson et al. and Atkinson et al. do not enable protecting ongoing system integrity of a software product having a plurality of pieces, as taught and claimed by Applicants.

Only Applicants teach a manifest header including header attributes of the software product. Only Applicants teach a list including a plurality of manifest items stored with said manifest header; each manifest item identifying a corresponding piece of the software product; each manifest item including at least one attribute; and a manifest digital signature stored with said manifest header; said manifest header, said header attributes, each of said plurality of items, and each said item attribute included in said manifest digital signature, as recited in independent claims 1, 7, and 16, as amended.

Independent claim 7, as amended, and independent claim 16 further recite the steps of computing a digital signature of each signed piece of the software product; and storing each said computed digital signature with the signed piece of the software product and excluding each said computed digital signature from said product load manifest. Only Applicants teach these features of the computer implemented method and computer program product of the invention as recited in independent claims 7, and 16, as amended. The combined teachings of Apperson et al. and

-10-

Serial No. 09/957,421

Atkinson et al. do not disclose nor remotely suggest these expressly recited features of independent claims 7, and 16, as amended.

Thus, each of the independent claims 1, 7, and 16, as amended, is patentable.

Further as recited in dependent claims 5, 6, 10, 11, 12, 13, 14, 17, and 18, as amended, only Applicants teach creating an amended manifest for identifying added and deleted pieces of the software product, and generating a single linked list for chaining said amended manifest to said product load manifest.

Further as recited in dependent claim 3, only Applicants teach that a digital signature of said signed corresponding piece of the software product is stored with said signed corresponding piece of the software product and said signature is excluded from said manifest item identifying said signed corresponding piece of the software product. The combined teachings of Apperson et al. and Atkinson et al. do not disclose nor remotely suggest the subject matter of dependent claim 3, as amended.

Each of the dependent claims 2-6, 8-15, and 17-20, as amended, further defines the invention of patentable independent claims 1, 7, and 16, as amended, and each of the dependent claims 2-6, 8-15, and 17-20, as amended, is likewise patentable.

Applicants have reviewed all the art of record, and respectfully submit that the claimed invention is patentable over all the art of record, including the references not relied upon by the Examiner for the rejection of the pending claims.

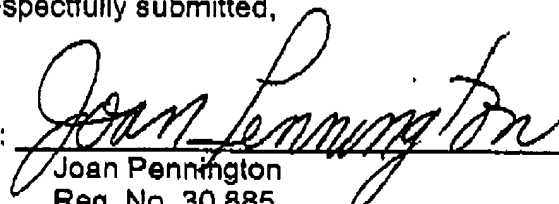It is believed that the present application is now in condition for allowance

-11-

Serial No. 09/957,421

and allowance of each of the pending claims 1-20, as amended, is respectfully requested. Prompt and favorable reconsideration is respectfully requested.

If the Examiner upon considering this amendment should find that a telephone interview would be helpful in expediting allowance of the present application, the Examiner is respectfully urged to call the applicants' attorney at the number listed below.

Respectfully submitted,

By: Joan Pennington
Joan Pennington
Reg. No. 30,885
Telephone: (312) 670-0736

-12-